

1 Keith A. Weaver  
Nevada Bar No. 10271  
2 Keith.Weaver@lewisbrisbois.com  
Nausheen K. Peters  
3 Nevada Bar No. 12984  
Nausheen.Peters@lewisbrisbois.com  
4 **LEWIS BRISBOIS BISGAARD & SMITH LLP**  
6385 S. Rainbow Boulevard, Suite 600  
5 Las Vegas, Nevada 89118  
Telephone: 702.893.3383  
6 Facsimile: 702.893.3789

7 Phyllis B. Sumner (*pro hac vice* forthcoming)  
Elizabeth D. Adler (*pro hac vice* forthcoming)  
8 James M. Brigman (*pro hac vice* forthcoming)  
**King & Spalding LLP**  
9 1180 Peachtree Street, NE, Suite 1600  
Atlanta, GA 30309  
10 (404) 572-4600  
psumner@kslaw.com  
11 eadler@kslaw.com  
mbrigman@kslaw.com

12 *Attorneys for Defendant*  
13 *ReproSource Fertility Diagnostics, Inc.*

14 **UNITED STATES DISTRICT COURT**  
15 **FOR THE DISTRICT OF NEVADA**

16 Lisa Gordon,

17 Plaintiff,

18 v.

19 ReproSource Fertility Diagnostics Inc.,

20 Defendant.

Case No.

**DEFENDANT REPROSOURCE  
FERTILITY DIAGNOSTICS, INC.'S  
NOTICE OF REMOVAL**

Complaint Filed: January 25, 2022

**PETITION FOR REMOVAL OF ACTION UNDER 28 U.S.C. §§ 1332, 1441, 1446, and 1453**

Defendant ReproSource Fertility Diagnostics, Inc. (“ReproSource”) hereby removes this purported class action from the Eighth Judicial District Court in Clark County, Nevada to the United States District Court for the District of Nevada. This Notice of Removal is filed pursuant to 28 U.S.C. §§ 1332, 1441, 1446, and 1453, and on the basis of the following facts, which show that this case may properly be removed to this Court:

**JURISDICTIONAL STATEMENT**

This Court has original jurisdiction over the the instant case pursuant to the Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119 Stat. 4 (codified in scattered sections of 28 U.S.C.) (“CAFA”). Here, the putative class contains at least 100 class members; any member of the putative class is a citizen of a State different from that of any defendant; and the amount in controversy exceeds \$5 million in the aggregate for the entire class, exclusive of interest and costs. 28 U.S.C. § 1332(d).

**I. BACKGROUND AND PLAINTIFFS’ COMPLAINT**

1. Plaintiff Lisa Gordon (“Plaintiff”) filed this case on January 25, 2022 in the Eighth Judicial District Court in Clark County, Nevada, Case Number A-22-847206-C, styled as *Lisa Gordon, individually and on behalf of all others similarly situated v. ReproSource Fertility Diagnostics Inc.* (the “State Court Action”).

2. The Complaint filed in the State Court Action is attached as Exhibit A (the “Complaint” or “Compl.”). ReproSource was served with the Complaint on January 28, 2022.

3. The Complaint asserts the following claims: (1) negligence, (2) invasion of privacy; (3) breach of contract; (4) breach of implied contract; and (5) violation of NRS 598. *See* Compl. ¶¶ 53-105.

4. The foregoing claims all arise from the ransomware security incident that occurred in August 2021. *See id.* ¶ 3.

5. As set forth in the Complaint, Plaintiff alleges criminals accessed her personal information and that she is at increased risk of identity theft and fraud. *See id.* ¶ 5, 29.

1           6.       Plaintiff alleges that ReproSource failed to protect her personal information and  
2 caused an invasion of her privacy. *See id.* ¶ 31.

3           7.       Plaintiff also alleges that ReproSource offered one-year of identity theft protection  
4 through a third-party vendor, but that this protection is inadequate. *See id.* ¶ 30, 40.

5           8.       Plaintiff seeks to certify a nationwide class of “[a]ll persons whose sensitive personal  
6 information, including, but not limited to, names, home addresses, dates of birth, driver’s licenses,  
7 and social security numbers was obtained by an unauthorized individual or individuals from  
8 Defendant during the August 2021 data breach.” *Id.* ¶ 42.

9           9.       Plaintiff requests the following relief:

10           a.       Equitable relief enjoining ReproSource from engaging in its acts and omissions  
11 leading to the disclosure of Plaintiff’s information. *See id.* ¶ 106.

12           b.       Compensatory damages to redress Plaintiff’s alleged damages, in the form of direct  
13 identity theft, identity theft, expenses for credit monitoring and identity theft  
14 insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and  
15 other economic and non-economic harm. *Id.*

16           c.       Statutory and nominal damages. *Id.*

17           d.       “[I]njunctive relief including, without limitation, (i) adequate credit monitoring, (ii)  
18 adequate identity theft insurance, (iii) instituting security protocols in compliance  
19 with the appropriate standards and (iv) requiring Defendant to submit to periodic  
20 compliance audits by a third party regarding the security of personal identifying  
21 information in its possession, custody and control.” *Id.*

22           e.       An award of Plaintiff and the Class Members interest, costs and attorneys’ fees. *Id.*

23           10.       Based on the allegations of the Complaint, this case is properly removed to this Court  
24 pursuant to 28 U.S.C. §§ 1441, 1446, and 1453 because ReproSource satisfied the procedural  
25 requirements for removal, and Plaintiff’s demands for relief indicate that this Court has subject  
26 matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d).

27       ///

28       ///

1 **II. THIS FEDERAL COURT HAS ORIGINAL JURISDICTION OVER THIS ACTION**  
 2 **UNDER CAFA**

3 11. This Court has original jurisdiction over the State Court Action, and the case may be  
 4 removed to this Court pursuant to the Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119  
 5 Stat. 4 (codified in scattered sections of 28 U.S.C.) (“CAFA”).

6 12. CAFA reflects Congress’s intent to have federal courts adjudicate substantial class  
 7 action suits brought against out-of-state defendants. To that end, CAFA provides that class actions  
 8 filed in state court are removable to federal court if they meet certain basic prerequisites.  
 9 Specifically, CAFA expanded federal jurisdiction over class actions by amending 28 U.S.C. § 1332  
 10 to grant original jurisdiction where the putative class contains at least 100 class members; any  
 11 member of the putative class is a citizen of a State different from that of any defendant; and the  
 12 amount in controversy exceeds \$5 million in the aggregate for the entire class, exclusive of interest  
 13 and costs. 28 U.S.C. § 1332(d).

14 **A. The Putative Class Exceeds 100 Members.**

15 13. Plaintiff purports to assert claims on behalf of “[a]ll persons whose sensitive personal  
 16 information . . . was obtained by an unauthorized individual or individuals from Defendant during  
 17 the August 2021 data breach. *Id.* ¶ 42.

18 14. Plaintiff alleges that the putative class is comprised of over 3,000 persons. *Id.* ¶ 44.

19 15. Accordingly, the aggregate number of putative class members is greater than 100 for  
 20 purposes of 28 U.S.C. § 1332(d)(5)(B).

21 **B. Minimal Diversity Exists.**

22 16. Under CAFA, only minimal diversity is required to confer original federal  
 23 jurisdiction. *See* 28 U.S.C. § 1332(d)(2)(A) (“The district courts shall have original jurisdiction of  
 24 any civil action in which the matter in controversy exceeds the sum or value of \$5,000,000, exclusive  
 25 of interest and costs, and is a class action in which . . . *any member of a class of plaintiffs is a citizen*  
 26 *of a State different from any defendant[.]*”) (emphasis added).

27 17. This element is satisfied. ReproSource is a Massachusetts Corporation with its  
 28 principal place of business in Massachusetts.

1 18. Plaintiff is a Nevada resident. Compl. ¶ 12.

2 19. Because at least one member of the putative class (*i.e.*, Plaintiff and all class members  
3 who are not Massachusetts residents) is diverse from ReproSource, the requirement of minimal  
4 diversity under 28 U.S.C. § 1332(d)(2)(A) is satisfied.

5 **C. The Amount in Controversy Exceeds \$5 Million.**

6 20. Under CAFA, federal district courts have original jurisdiction where, among other  
7 things, the “matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and  
8 costs.” 28 U.S.C. § 1332(d)(2).

9 21. To satisfy this requirement, a defendant’s notice of removal “need not contain  
10 evidentiary submissions”; all that is required is “a plausible allegation that the amount in controversy  
11 exceeds the jurisdictional threshold.” *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S.  
12 81, 84, 89 (2014). *See also Greene v. Harley-Davidson, Inc.*, 965 F.2d 767, 772 (9th Cir. 2020)  
13 (CAFA’s amount-in-controversy requirement is satisfied where “it is reasonably possible that the  
14 potential liability exceeds \$5 million”).

15 22. Further, where a “plaintiff’s complaint does not state the amount in controversy, the  
16 defendant’s notice of removal may do so.” *Dart*, 574 U.S. at 84.

17 23. The Complaint filed by Plaintiffs in the State Court Action does not specify a precise  
18 amount of claimed damages. But it is clear from Plaintiffs’ allegations that Plaintiff seeks to recover  
19 far more than \$5 million in relief from ReproSource.

20 24. Plaintiff seeks, among other things (i) equitable relief enjoining ReproSource from  
21 engaging in its acts and omissions leading to the disclosure of Plaintiff’s information, Compl. ¶ 106;  
22 (ii) compensatory damages to redress Plaintiff’s alleged damages, in the form of direct identity theft,  
23 identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses,  
24 anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, *id.*; (iii)  
25 statutory and nominal damages, *id.*; “injunctive relief including, without limitation, (i) adequate  
26 credit monitoring, (ii) adequate identity theft insurance, (iii) instituting security protocols in  
27 compliance with the appropriate standards and (iv) requiring Defendant to submit to periodic  
28

1 compliance audits by a third party regarding the security of personal identifying information in its  
2 possession, custody and control.” *Id.*

3 25. Considering only Plaintiff’s claim for “adequate credit monitoring” and “adequate  
4 identity theft insurance” the \$5 million amount-in-controversy requirement is satisfied.

5 26. Plaintiff alleges that “Plaintiff and thousands of Class Members received letters from  
6 Defendant notifying them that it learned of suspicious activity that allowed one or more  
7 cybercriminals to access its systems through a ransomware attack.” *Id.* ¶ 28.

8 27. As a result of the security incident described in the Complaint, ReproSource provided  
9 written notice to in excess of 220,000 individuals stating that ReproSource had been the victim of a  
10 security incident in which those customers’ personally identifying information may have been  
11 accessed by an unauthorized actor. *See* Exhibit B at 2.

12 28. In the aftermath of the security incident described in the Complaint, ReproSource  
13 retained Kroll Information Assurance, LLC to offer credit monitoring to all potentially impacted  
14 individuals. The value of the credit monitoring offered to all potentially impacted individuals by  
15 ReproSource was \$35.05 per-person. *See* Exhibit B, Declaration of Keena Hausmann at 2.

16 29. Plaintiff alleges that this protection was inadequate. *See* Compl. ¶¶ 30, 36, 40.

17 30. Thus, the amount in controversy based on a 220,000 person class<sup>1</sup> would be \$7.71  
18 million (220,000 \* \$35.05 = \$7,711,000).

19 31. The credit protection is only one among many forms of relief Plaintiffs seek. As  
20 noted above, the Complaint alleges Plaintiff is entitled to compensatory, statutory, and nominal  
21 damages. Plaintiff also seeks broad injunctive relief and attorneys’ fees.

22 32. It is therefore likely that Plaintiffs seek more in damages than the calculation above—  
23 which is based on only one alleged injury—would suggest.

24 33. Accordingly, the amount-in-controversy element is met.

25 \_\_\_\_\_  
26 <sup>1</sup> “In any class action, the claims of the individual class members shall be aggregated to determine  
27 whether the matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and  
28 costs.” 28 U.S.C. § 1332(d)(6).

1 **III. THE PROCEDURAL REQUIREMENTS FOR REMOVAL ARE SATISFIED**

2 34. ReproSource is removing the State Court Action to the United States District Court  
3 for the District of Nevada because the case was originally filed in the Eighth Judicial District, Clark  
4 County Nevada, a state court located within the District of Nevada. Accordingly, this Court is in  
5 the “district and division embracing the place where [the] action is pending.” 28 U.S.C. § 1441(a).

6 35. Removal is also timely. Plaintiffs filed the State Court Action on January 25, 2022.  
7 ReproSource was served on January 28, 2022. Accordingly, this Notice of Removal was filed within  
8 30 days of the service of the Complaint on ReproSource, making removal timely under 28 U.S.C. §  
9 1446(b). *See Murphy Bros., Inc. v. Michetti Pipestringing, Inc.*, 526 U.S. 344, 347-48 (1999). No  
10 previous application has been made for the relief requested herein.

11 36. ReproSource has not filed a responsive pleading, and it reserves all rights to assert  
12 any and all defenses with respect to the Complaint. ReproSource also reserves the right to amend  
13 or supplement this Notice.

14 37. Pursuant to 28 U.S.C. § 1446(a), “a copy of all process, pleadings, and orders served”  
15 on ReproSource is attached as Exhibit A. Pursuant to 28 U.S.C. § 1446(d), a copy of this Notice is  
16 being served upon counsel for Plaintiff, and a copy is being filed with the Eighth Judicial District  
17 Court, Clark County, Nevada.

18 38. For the foregoing reasons, this action is properly removed to this Court pursuant to  
19 28 U.S.C. §§ 1441, 1446 and 1453, and this Court may exercise jurisdiction over this matter pursuant  
20 to 28 U.S.C. § 1332(d).

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

1 **IV. CONCLUSION**

2 WHEREFORE, ReproSource removes this action from the Eighth Judicial District Court,  
3 Clark County, Nevada to the United States District Court for the District of Nevada pursuant to 28  
4 U.S.C. §§ 1332(d), 1441, 1446, and 1453(b).

5 Respectfully submitted this 24th day of February 2022.

6  
7 /s/ Keith A. Weaver

8 Keith A. Weaver

9 Nevada Bar No. 10271

Keith.Weaver@lewisbrisbois.com

10 Nausheen K. Peters

Nevada Bar No. 12984

Nausheen.Peters@lewisbrisbois.com

11 **LEWIS BRISBOIS BISGAARD & SMITH LLP**

6385 S. Rainbow Boulevard, Suite 600

12 Las Vegas, Nevada 89118

Telephone: 702.893.3383

13 Facsimile: 702.893.3789

14 Phyllis B. Sumner (*pro hac vice* forthcoming)

15 Elizabeth D. Adler (*pro hac vice* forthcoming)

16 James M. Brigman (*pro hac vice* forthcoming)

King & Spalding LLP

1180 Peachtree Street, NE, Suite 1600

17 Atlanta, GA 30309

(404) 572-4600

18 psumner@kslaw.com

eadler@kslaw.com

19 mbrigman@kslaw.com

20 *Attorneys for Defendant*

21 *ReproSource Fertility Diagnostics, Inc.*



**CERTIFICATE OF SERVICE**

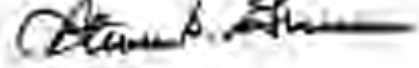
I hereby certify that on this 24<sup>th</sup> day of February, 2022, a true and correct copy of the foregoing has been served via E-mail and U.S. Postal Service by first class, registered, or certified mail delivery:

George Haines, Esq.  
Gerardo Avalos, Esq.  
**FREEDOM LAW FIRM, LLC**  
8985 South Eastern Ave., Suite 350  
Las Vegas, NV 89123  
Phone: (702) 880-5554  
FAX: (702) 385-5518  
Email: [info@freedomlegalteam.com](mailto:info@freedomlegalteam.com)

Michael Kind, Esq.  
**KIND LAW**  
8860 South Maryland Parkway, Suite 106  
Las Vegas, Nevada 89123  
(702) 337-2322  
(702) 329-5881 (fax)  
[mk@kindlaw.com](mailto:mk@kindlaw.com)  
*Attorneys for Plaintiff Lisa Gordon  
and on behalf of all others similarly situated*

By /s/ Jeannette Versoza  
An Employee of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

# EXHIBIT A



George Haines, Esq.  
Nevada Bar No. 9411  
Gerardo Avalos, Esq.  
Nevada Bar No. 15171  
**FREEDOM LAW FIRM, LLC**  
8985 South Eastern Ave., Suite 350  
Las Vegas, NV 89123  
Phone: (702) 880-5554  
FAX: (702) 385-5518  
Email: info@freedomlegalteam.com

CASE NO: A-22-847206-C  
Department 26

Michael Kind, Esq.  
Nevada Bar No.: 13903  
**KIND LAW**  
8860 South Maryland Parkway, Suite 106  
Las Vegas, Nevada 89123  
(702) 337-2322  
(702) 329-5881 (fax)  
mk@kindlaw.com  
*Attorneys for Plaintiff Lisa Gordon  
and on behalf of all others similarly situated*

**EIGHTH JUDICIAL DISTRICT COURT  
CLARK COUNTY, NEVADA**

Lisa Gordon, individually  
and on behalf of all others  
similarly situated,

Plaintiff,

v.

ReproSource Fertility  
Diagnostics Inc.

Defendant.

Case No.: \_\_\_\_\_

Dept. No.: \_\_\_\_\_

**Class Action**

**Complaint for Damages based on:  
(1) Negligence; (2) Invasion of  
Privacy; (3) Breach of Contract; (4)  
Breach of Implied Contract; and  
(5) Violation of NRS 598**

**Jury Trial Demanded**

**EXEMPT FROM ARBITRATION**

## INTRODUCTION

1. Defendant ReproSource Fertility Diagnostics, Inc., (“Defendant”) failed to safeguard the confidential personal identifying information of thousands of individuals (hereinafter referred to as the “Class” or “Class Members”). This class action is brought on behalf of patients who’s personally identifiable information (“PII” or “Private Information”) was stolen by cybercriminals in a cyber-attack that accessed sensitive patient information through ReproSource’s services.
2. On or sometime prior to August 8, 2021, a group of cybercriminals gained access to certain files on Defendant’s computer network and servers containing personal information belonging to the Class Members.
3. Plaintiff and Class Members were not notified of the data breach until December 17, 2021, more than three months after her information was first accessed.
4. The cybercriminals accessed insufficiently protected information belonging to Plaintiff and the Class Members. Upon information and belief, as a result of Defendant’s failure to properly secure Plaintiff’s and the Class Members’ personal information, the cybercriminals obtained extensive personal information including names, addresses, email addresses, dates of birth, Social Security numbers, health insurance billing information, and treating physician information, collectively known as personally identifiable information (“PII” or “Private Information”).
5. As a result of Defendant’s actions, Plaintiff and the Class Members were harmed and forced to take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all of the Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized credit card charges, unauthorized

1 access to email accounts, identity theft, and other fraudulent use of their  
2 financial accounts.

3 6. Defendant's wrongful actions and/or inaction constitute common law  
4 negligence, invasion of privacy by the public disclosure of private facts, breach  
5 of contract, and breach of implied contract.

6 7. Plaintiff, on behalf of herself, and the Class seeks (i) actual damages, economic  
7 damages, emotional distress damages, statutory damages and/or nominal  
8 damages, (ii) exemplary damages, (iii) injunctive relief, and (iv) attorneys'  
9 fees, litigation expenses and costs.

#### 10 JURISDICTION AND VENUE

11 8. This Court has jurisdiction to hear this case.

12 9. Plaintiff is a resident of Clark County, Nevada. Defendant is a corporation  
13 organized and existing by virtue of the laws of the State of Nevada and  
14 registered with the Nevada Secretary of State. Defendant conducts business in  
15 the State of Nevada, County of Clark.

16 10. The transactions and occurrences that give rise to Plaintiff's claims against  
17 Defendant occurred in Clark County, Nevada.

18 11. Therefore, the Eighth Judicial District Court, Clark County, Nevada has  
19 personal jurisdiction over both Plaintiff and Defendant and subject matter  
20 jurisdiction pursuant to Article 6, Section 6 of the Nevada Constitution and  
21 NRS 4.370.

#### 22 PARTIES

23 12. Plaintiff Lisa Gordon ("Gordon") is a natural person residing in Clark County,  
24 Nevada.

25 13. Defendant ReproSource is a fertility testing company, which operates  
26 nationally, including in Nevada. ReproSource offers a number of fertility  
27 treatment products, including egg supply testing, semen testing, recurrent  
28

1 pregnancy loss laboratory testing services, and other fertility-focused  
2 services.

3 **FACTUAL ALLEGATIONS**

4 14. Identity theft, which costs Americans billions of dollars a year, occurs when an  
5 individual's personal identifying information is used without his or her  
6 permission to commit fraud or other crimes. Victims of identity theft typically  
7 lose hundreds of hours dealing with the crime, and they typically lose hundreds  
8 of dollars.

9 15. According to the Federal Trade Commission ("FTC"):

10 Identity theft is serious. While some identity theft victims can  
11 resolve their problems quickly, others spend hundreds of dollars  
12 and many days repairing damage to their good name and credit  
13 record. Some consumers victimized by identity theft may lose out  
14 on job opportunities, or be denied loans for education, housing or  
15 cars because of negative information on their credit reports. In  
16 rare cases, they may even be arrested for crimes they did not  
17 commit.

18 16. The United States Government Accountability Office ("GAO") has stated that  
19 identity thieves can use identifying data to open financial accounts and incur  
20 charges and credit in a person's name. As the GAO has stated, this type of  
21 identity theft is the most damaging because it may take some time for the victim  
22 to become aware of the theft and can cause significant harm to the victim's  
23 credit rating. Like the FTC, the GAO explained that victims of identity theft  
24 face "substantial costs and inconvenience repairing damage to their credit  
25 records," as well the damage to their "good name."

26 17. Healthcare Industry Standards highlights several basic cybersecurity  
27 safeguards that can be implemented to improve cyber resilience that require a  
28 relatively small financial investment yet can have a major impact on an

organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices

18. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

19. Accordingly, Federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed by Defendant.

20. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

- a. Know what personal information you have in your files and on your computers;
- b. Keep only what you need for your business;
- c. Protect the information that you keep;
- d. Properly dispose of what you no longer need;
- e. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and
- f. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

1 Keith A. Weaver  
Nevada Bar No. 10271  
2 Keith.Weaver@lewisbrisbois.com  
Nausheen K. Peters  
3 Nevada Bar No. 12984  
Nausheen.Peters@lewisbrisbois.com  
4 **LEWIS BRISBOIS BISGAARD & SMITH LLP**  
6385 S. Rainbow Boulevard, Suite 600  
5 Las Vegas, Nevada 89118  
Telephone: 702.893.3383  
6 Facsimile: 702.893.3789

7 Phyllis B. Sumner (*pro hac vice* forthcoming)  
Elizabeth D. Adler (*pro hac vice* forthcoming)  
8 James M. Brigman (*pro hac vice* forthcoming)  
**King & Spalding LLP**  
9 1180 Peachtree Street, NE, Suite 1600  
Atlanta, GA 30309  
10 (404) 572-4600  
psumner@kslaw.com  
11 eadler@kslaw.com  
mbrigman@kslaw.com

12 *Attorneys for Defendant*  
13 *ReproSource Fertility Diagnostics, Inc.*

14 **UNITED STATES DISTRICT COURT**  
15 **FOR THE DISTRICT OF NEVADA**

16 Lisa Gordon,

17  
18 Plaintiff,

19 v.

20 ReproSource Fertility Diagnostics Inc.,

21 Defendant.  
22  
23  
24  
25  
26  
27  
28

Case No.

**DEFENDANT REPROSOURCE  
FERTILITY DIAGNOSTICS, INC.'S  
CERTIFICATE OF INTERESTED  
PARTIES**

Complaint Filed: January 25, 2022



COMES NOW Defendant ReproSource Fertility Diagnostics, Inc., by and through its counsel of record, hereby provides the following disclosure pursuant to FRCP 7.1.

The undersigned, attorney of record for ReproSource Fertility Diagnostics Inc., certifies that the following may have a direct, pecuniary interest in the outcome of this case: Quest Diagnostics, Inc. owns 10% or more of the stock in ReproSource Fertility Diagnostics, Inc. Quest Diagnostics, Inc. is publicly traded on the New York Stock Exchange (ticker symbol: DGX).

These representations are made to enable judges of the court to evaluate possible disqualifications or recusal.

Respectfully submitted this 24th day of February 2022.

/s/ Keith A. Weaver

Keith A. Weaver

Nevada Bar No. 10271

Keith.Weaver@lewisbrisbois.com

Nausheen K. Peters

Nevada Bar No. 12984

Nausheen.Peters@lewisbrisbois.com

**LEWIS BRISBOIS BISGAARD & SMITH LLP**

6385 S. Rainbow Boulevard, Suite 600

Las Vegas, Nevada 89118

Telephone: 702.893.3383

Facsimile: 702.893.3789

Phyllis B. Sumner (*pro hac vice* forthcoming)

Elizabeth D. Adler (*pro hac vice* forthcoming)

James M. Brigman (*pro hac vice* forthcoming)

King & Spalding LLP

1180 Peachtree Street, NE, Suite 1600

Atlanta, GA 30309

(404) 572-4600

psumner@kslaw.com

eadler@kslaw.com

mbrigman@kslaw.com

*Attorneys for Defendant*

*ReproSource Fertility Diagnostics, Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 24<sup>th</sup> day of February, 2022, a true and correct copy of the foregoing has been served via E-mail and U.S. Postal Service by first class, registered, or certified mail delivery:

George Haines, Esq.  
Gerardo Avalos, Esq.  
**FREEDOM LAW FIRM, LLC**  
8985 South Eastern Ave., Suite 350  
Las Vegas, NV 89123  
Phone: (702) 880-5554  
FAX: (702) 385-5518  
Email: [info@freedomlegalteam.com](mailto:info@freedomlegalteam.com)

Michael Kind, Esq.  
**KIND LAW**  
8860 South Maryland Parkway, Suite 106  
Las Vegas, Nevada 89123  
(702) 337-2322  
(702) 329-5881 (fax)  
[mk@kindlaw.com](mailto:mk@kindlaw.com)  
*Attorneys for Plaintiff Lisa Gordon  
and on behalf of all others similarly situated*

By /s/ Jeannette Versoza  
An Employee of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

- 1 21. The FTC Report also instructs companies that outsource any business functions  
2 to proactively investigate the data security practices of the outsourced company  
3 and examine their standards.
- 4 22. Title II of HIPAA contains what are known as the Administrative  
5 Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require,  
6 among other things, that the Department of Health and Human Services  
7 (“HHS”) create rules to streamline the standards for handling Private  
8 Information like the data Defendant left unguarded. The HHS has subsequently  
9 promulgated five rules under authority of the Administrative Simplification  
10 provisions of HIPAA.
- 11 23. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required  
12 Defendant to provide notice of the breach to each affected individual “without  
13 unreasonable delay and in no case later than 60 days following discovery of the  
14 breach.”
- 15 24. HIPPA requires covered entities like ReproSource protect against reasonably  
16 anticipated threat to the security of Private Information. Covered entities must  
17 implement safeguards to ensure the confidentiality, integrity, and availability  
18 of PII. Safeguards must include physical, technical, and administrative  
19 components.
- 20 25. Defendant’s Data Breach resulted from a combination of insufficiencies that  
21 demonstrate Defendant failed to comply with safeguards mandated by HIPAA  
22 regulations.
- 23 26. The Federal Trade Commission (“FTC”) has concluded that a company’s  
24 failure to maintain reasonable and appropriate data security for consumers’  
25 sensitive personal information is an “unfair practice” in violation of the FTC  
26 Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir.  
27 2015).
- 28

1 27. Upon information and belief, Defendant has policies and procedures in place  
2 regarding the safeguarding of confidential information it is entrusted with and  
3 Defendant failed to comply with those policies. Defendant also negligently  
4 failed to comply with industry standards or even implement rudimentary  
5 security practices, resulting in the Plaintiff's and the Class' confidential  
6 information being substantially less safe than had this information been  
7 entrusted with other similar companies.

8 28. In or around December 2021, Plaintiff and thousands of Class Members  
9 received letters from Defendant notifying them that it learned of suspicious  
10 activity that allowed one or more cybercriminals to access its systems through  
11 a ransomware attack. The December 2021 Notice disclosed that a ransomware  
12 attacks enabled a threat actor to access ReproSource systems.

13 29. The criminals were able to access Plaintiff's personal information because  
14 Defendant failed to take reasonable measures to protect the Personally  
15 Identifiable Information it collected and stored. Among other things, Defendant  
16 failed to implement data security measures designed to prevent this attack,  
17 despite repeated warnings to the healthcare industry, insurance companies, and  
18 associated entities about the risk of cyberattacks and the highly publicized  
19 occurrence of many similar attacks in the recent past on other healthcare  
20 providers.

21 30. ReproSource's notice of Data Breach was not just untimely but woefully  
22 deficient, failing to provide basic details, including but not limited to, how  
23 unauthorized parties accessed its networks, whether the information was  
24 encrypted or otherwise protected, how it learned of the Data Breach, whether  
25 the breach occurred system-wide, whether servers storing information were  
26 accessed, and how many patients were affected by the Data Breach. Even  
27 worse, ReproSource offered only one year of identity monitoring to Plaintiff  
28

1 and Class members, which required the disclosure of additional PII that  
2 ReproSource had just demonstrated it could not be trusted with.

3 31. As a result of Defendant's failure to properly secure Plaintiff's and the Class  
4 Members' personal identifying information, Plaintiff's and the Class Members'  
5 privacy has been invaded.

6 32. Moreover, all of this personal information is likely for sale to criminals on the  
7 dark web, meaning that unauthorized parties have accessed and viewed  
8 Plaintiff's and Class members' unencrypted, unredacted information, including  
9 names, addresses, email addresses, dates of birth, Social Security numbers,  
10 member ID numbers, policyholder names, employer names, policy numbers,  
11 and more.

12 33. Given all of the information obtained, the criminals would also be able to create  
13 numerous fake accounts and sell sensitive health information, as part of their  
14 identity theft operation.

15 34. As a direct and proximate result of Defendant's wrongful disclosure, criminals  
16 now have Plaintiff's and the Class Members' personal identifying information.  
17 Additionally, the disclosure makes Plaintiff and Class Members much more  
18 likely to respond to requests from Defendant or law enforcement agencies for  
19 more personal information, such as bank account numbers, login information  
20 or even Social Security numbers. Because criminals know this and are capable  
21 of posing as Defendant or law enforcement agencies, consumers like Plaintiff  
22 and their fellow Class Members are more likely to unknowingly give away their  
23 sensitive personal information to other criminals.

24 35. Medical identity theft can result in inaccuracies in medical records and costly  
25 false claims. It can also have life-threatening consequences. If a victim's health  
26 information is mixed with other records, it can lead to misdiagnosis or  
27 mistreatment. "Medical identity theft is a growing and dangerous crime that  
28

1 leaves its victims with little to no recourse for recovery,” reported Pam Dixon,  
2 executive director of World Privacy Forum.

3 36. Defendant’s wrongful actions and inaction here directly and proximately  
4 caused the public disclosure of Plaintiff’s and Class Members’ personal  
5 identifying information without their knowledge, authorization and/or consent.  
6 As a further direct and proximate result of Defendant’s wrongful actions and/or  
7 inaction, Plaintiff and Class Members have suffered, and will continue to  
8 suffer, damages including, without limitation, expenses for credit monitoring  
9 and identity theft insurance, out-of-pocket expenses, anxiety, emotional  
10 distress, loss of privacy, and other economic and non-economic harm.

11 37. Plaintiff and Class Members are now required to monitor their accounts and to  
12 respond to identity theft. Plaintiff and Class Members now face a very high risk  
13 of identity theft.

14 38. Names and dates of birth, combined with contact information like telephone  
15 numbers and email addresses, are very valuable to hackers and identity thieves  
16 as it allows them to access users’ other accounts. Thus, even if payment card  
17 information were not involved in the Data Breach, the unauthorized parties  
18 could use Plaintiff’s and Class members’ Private Information to access  
19 accounts, including, but not limited to email accounts and financial accounts,  
20 to engage in the fraudulent activity identified by Plaintiff.

21 39. Despite disregarding its obligations to protect the sensitive information that  
22 Plaintiff and Class Members entrusted it with, Defendant has not offered  
23 Plaintiff and Class Members any monetary compensation.

24 40. Defendant has offered identity protection, but only for one year, and only if the  
25 Plaintiff and Class Members have access to a computer, internet services,  
26 established credit, and are enrolled in those identity protection services by  
27 March 16, 2022. Plaintiff’s and Class Member’s personal information has been  
28 disclosed to criminal entities who may wait the one year mark and begin to use

Plaintiff and Class Members' personal information. Additionally, certain Class Members may be prevented from enrolling in the identity protection services due to a lack of access to a computer with internet services or bad credit.

41. ReproSource was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. ReproSource was also aware of the significant repercussions that would result from its failure to do so.

### CLASS ACTION ALLEGATIONS

42. Pursuant to Rule 23 of the Nevada Rules of Civil Procedure, Plaintiff brings this class action on behalf of herself and the following Class of similarly situated individuals:

All persons whose sensitive personal information, including, but not limited to, names, home addresses, dates of birth, driver's licenses, and social security numbers was obtained by an unauthorized individual or individuals from Defendant during the August 2021 data breach.

43. The Class specifically excludes Defendant and its officers, directors, agents and/or officers, the Court and Court personnel.

44. The putative Class is comprised of over 3,000 persons, making joinder impracticable. The joinder of the Class members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the Court. The Class can be identified through Defendant's records or Defendant's agents' records.

45. The rights of each Class Member were violated in an identical manner as a result of Defendant's willful, reckless and/or negligent actions and/or inaction.

1 46. The questions of law and fact common to all Class Members, and which  
2 predominate over any questions affecting only individual Class Members, are  
3 as follows:

- 4 a. Whether Defendant negligently failed to maintain and execute reasonable  
5 procedures designed to prevent unauthorized access to Plaintiff's and Class  
6 Members' personal identifying information;
- 7 b. Whether Defendant was negligent in storing and failing to adequately  
8 safeguard Plaintiff's and Class Members' personal identifying information;
- 9 c. Whether Defendant owed a duty to Plaintiff and Class Members to exercise  
10 reasonable care in protecting and securing their personal identifying  
11 information;
- 12 d. Whether Defendant breached its duties to exercise reasonable care in failing  
13 to protect and secure Plaintiff's and Class Members' personal identifying  
14 information;
- 15 e. Whether by disclosing Plaintiff's and Class Members' personal identifying  
16 information without authorization, Defendant invaded Plaintiff's and Class  
17 Members' privacy;
- 18 f. Whether Defendant created an implied contract with Plaintiff and Class  
19 Members to keep their personal identifying information confidential; and
- 20 g. Whether Plaintiff and Class Members sustained damages as a result of  
21 Defendant's failure to secure and protect their personal identifying  
22 information.

23 47. Plaintiff and her counsel will fairly and adequately represent the interests of  
24 Class Members. Plaintiff has no interests antagonistic to, or in conflict with,  
25 Class Members' interests. Plaintiff's attorneys are highly experienced in the  
26 prosecution of consumer class action, complex litigation and privacy breach  
27 cases.  
28



1 48. Plaintiff's claims are typical of Class Members' claims in that Plaintiff's claims  
2 and Class Members' claims all arise from Defendant's wrongful disclosure of  
3 their personal identifying information and from Defendant's failure to properly  
4 secure and protect the same.

5 49. A class action is superior to all other available methods for fairly and efficiently  
6 adjudicating Plaintiff's and Class Members' claims. Plaintiff and Class  
7 Members have been irreparably harmed as a result of Defendant's wrongful  
8 actions and/or inaction. Litigating this case as a class action will reduce the  
9 possibility of repetitious litigation relating to Defendant's failure to secure and  
10 protect Plaintiff's and Class Members' personal identifying information.

11 50. Class certification, therefore, is appropriate pursuant to Rule 23 because the  
12 above common questions of law or fact predominate over any questions  
13 affecting individual Class Members, and a class action is superior to other  
14 available methods for the fair and efficient adjudication of this controversy.

15 51. Class certification also is appropriate pursuant to Rule 23 of the Nevada Rules  
16 of Civil Procedure because Defendant has acted or refused to act on grounds  
17 generally applicable to the Class, so that final injunctive relief or corresponding  
18 declaratory relief is appropriate as to the Class as a whole.

19 52. The expense and burden of litigation would substantially impair the ability of  
20 Class Members to pursue individual lawsuits in order to vindicate their rights.  
21 Absent a class action, Defendant will retain the benefits of their wrongdoing  
22 despite its serious violations of the law.

### 23 **FIRST CAUSE OF ACTION**

#### 24 **NEGLIGENCE**

25 53. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

26 54. Upon Defendant's accepting and storing the Private Information of Plaintiff  
27 and the Class in its computer systems and on its networks, Defendant undertook  
28 and owed a duty to Plaintiff and the Class to exercise reasonable care to secure

1 and safeguard that information and to use commercially reasonable methods to  
2 do so. Defendant knew that the Private Information was private and  
3 confidential and should be protected as private and confidential.

4 55. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private  
5 Information to an unreasonable risk of exposure and theft because Plaintiff and  
6 the Class were foreseeable and probable victims of any inadequate security  
7 practices.

8 56. It was reasonably foreseeable that Defendant's failure to exercise reasonable  
9 care in safeguarding and protecting Plaintiff's and Class Members' personal  
10 identifying information would result in an unauthorized third party gaining  
11 access to such information for no lawful purpose, and that such third parties  
12 would use Plaintiff's and Class Members' personal identifying information for  
13 malevolent and unlawful purposes, including the commission of direct theft and  
14 identity theft.

15 57. Defendant knew, or should have known, of the risks inherent in collection and  
16 storing Private Information and the importance of adequate security. Defendant  
17 knew of should have known about numerous well-publicized data breaches  
18 within the medical industry.

19 58. Plaintiff and the Class Members were (and continue to be) damaged as a direct  
20 and proximate result of Defendant's failure to secure and protect their personal  
21 identifying information as a result of, *inter alia*, direct theft, identity theft,  
22 expenses for credit monitoring and identity theft herein, insurance incurred in  
23 mitigation, out-of-pocket expenses, anxiety, emotional distress, loss of privacy,  
24 and other economic and non-economic harm, for which they suffered loss and  
25 are entitled to compensation.

26 59. Defendant's wrongful actions and/or inaction (as described above) constituted  
27 (and continue to constitute) negligence at common law.

28 ///

1 **SECOND CAUSE OF ACTION**

2 **INVASION OF PRIVACY BY PUBLIC**

3 **DISCLOSURE OF PRIVATE FACTS AND INTRUSION UPON SECLUSION**

4 60. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

5 61. Plaintiff's and Class Members' personal identifying information is and always  
6 has been private information.

7 62. Dissemination of Plaintiff's and Class Members' personal identifying  
8 information is not of a legitimate public concern; publication to third parties of  
9 their personal identifying information would be, is and will continue to be,  
10 offensive to Plaintiff, Class Members, and other reasonable people.

11 63. Plaintiff and the Class Members were (and continue to be) damaged as a direct  
12 and proximate result of Defendant's invasion of their privacy by publicly  
13 disclosing their private facts including, *inter alia*, direct theft, identity theft,  
14 expenses for credit monitoring and identity theft insurance, out-of-pocket  
15 expenses, anxiety, emotional distress, loss of privacy, and other economic and  
16 non-economic harm, for which they are entitled to compensation. At the very  
17 least, Plaintiff and the Class Members are entitled to nominal damages.

18 64. Defendant's wrongful actions and/or inaction (as described above) constituted  
19 (and continue to constitute) an invasion of Plaintiff's and Class Members'  
20 privacy by publicly disclosing their private facts (*i.e.*, their personal identifying  
21 information).

22 **THIRD CAUSE OF ACTION**

23 **BREACH OF CONTRACT**

24 65. Plaintiff fully incorporates by reference all of the above paragraphs, as though  
25 fully set forth herein.

26 66. Plaintiff and other Class members entered into valid and enforceable express  
27 contracts with Defendant under which Plaintiff and other Class members  
28 agreed to provide their Private Information to Defendant, and Defendant

1 agreed to provide testing services and, impliedly, if not explicitly, agreed to  
2 protect Plaintiff's and Class members' Private Information.

3 67. These contracts include HIPAA privacy notices and explanation of benefits  
4 documents.

5 68. To the extent Defendant's obligation to protect Plaintiffs' and other Class  
6 Members' Private Information was not explicit in those express contracts, the  
7 express contracts included implied terms requiring Defendant to implement  
8 data security adequate to safeguard and protect the confidentiality of  
9 Plaintiffs' and other Class members' Private Information, including in  
10 accordance with HIPAA regulations; federal, state and local laws; and  
11 industry standards. Neither Plaintiff nor any Class member would have  
12 entered into these contracts with Defendant without understanding that  
13 Plaintiff's and other Class members' Private Information would be  
14 safeguarded and protected; stated otherwise, data security was an essential  
15 implied term of the parties' express contracts.

16 69. A meeting of the minds occurred, as Plaintiff and other Class members  
17 agreed, among other things, to provide their Private Information in exchange  
18 for Defendant's agreement to protect the confidentiality of that Private  
19 Information.

20 70. The protection of Plaintiff's and Class members' Private Information were  
21 material aspects of Plaintiff's and Class members' contracts with Defendant.

22 71. Defendant's promises and representations described above relating to HIPAA  
23 and industry practices, and Defendant's purported concern about its clients'  
24 privacy rights became terms of the contracts between Defendant and its  
25 clients, including Plaintiff and other Class members. Defendant breached  
26 these promises by failing to comply with HIPAA and reasonable industry  
27 practices.  
28

72. Plaintiff and Class members read, reviewed, and/or relied on statements made by or provided by ReproSource and/or otherwise understood that ReproSource would protect its patients' Private Information if that information were provided to ReproSource.

73. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

74. As a result of Defendant's breach of these terms, Plaintiff and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendant; the lost difference in the value between the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and other Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

75. Plaintiff and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

#### **FOURTH CAUSE OF ACTION**

##### **BREACH OF IMPLIED CONTRACT**

76. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

77. "Where the terms of a contract are literally complied with but one party to the contract deliberately contravenes the intention and spirit of the contract, that party can incur liability for breach of the implied covenant of good faith and

1 fair dealing.” *Hilton Hotels Corp. v. Butch Lewis Prods., Inc.*, 107 Nev. 226,  
2 232 (1991).

3 78. Among other things, Plaintiff and Class Members were required to disclose  
4 their personal identifying information to Defendant for the provision of  
5 healthcare services, as well as implied contracts for the Defendant to implement  
6 data security adequate to safeguard and protect the privacy of Plaintiff’s and  
7 Class members’ Private Information.

8 79. When Plaintiff and Class members provided their Private Information to  
9 Defendant in exchange for Defendant’s services, they entered into implied  
10 contracts with Defendant pursuant to which Defendant agreed to reasonably  
11 protect such information.

12 80. In entering into such implied contracts, Plaintiff and Class members reasonably  
13 believed and expected that Defendant’s data security practices complied with  
14 relevant laws and regulations and were consistent with industry standards.

15 81. Class members who paid money to Defendant reasonably believed and  
16 expected that Defendant would use part of those funds to obtain adequate data  
17 security. Defendant failed to do so.

18 82. Under implied contracts, Defendant and/or its affiliated providers promised and  
19 were obligated to: (a) provide fertility services to Plaintiff and Class members;  
20 and (b) protect Plaintiff’s and Class members’ Private Information provided to  
21 obtain the benefits of such services. In exchange, Plaintiff and Members of the  
22 Class agreed to pay money for these services, and to turn over their Private  
23 Information.

24 83. The implied contracts for the provision of fertility testing services—contracts  
25 that include the contractual obligations to maintain the privacy of Plaintiff’s  
26 and Class Members’ Private Information—are also acknowledged,  
27 memorialized, and embodied in multiple documents, including (among other  
28

documents) Defendant's Data Breach notification letter and Defendant's Notice of Privacy Practices.

84. Defendant's express representations, including, but not limited to the express representations found in its Notice of Privacy Practices, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information.

85. Plaintiff and class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

86. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

87. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class members' private information as set forth above.

88. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

89. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference

1 in the value between the healthcare with data security protection they paid for  
2 and the healthcare they received.

3 90. Had Defendant disclosed that its security was inadequate or that it did not  
4 adhere to industry-standard security measures, neither the Plaintiff, Class  
5 members, nor any reasonable person would have purchased healthcare from  
6 Defendant and/or its affiliated providers.

7 91. As a direct and proximate result of the Data Breach, Plaintiff and Class  
8 members have been harmed and suffered, and will continue to suffer, actual  
9 damages and injuries, including without limitation the release and disclosure of  
10 their Private Information, the loss of control of their Private Information, the  
11 imminent risk of suffering additional damages in the future, disruption of their  
12 medical care and treatment, out of pocket expenses, and the loss of the benefit  
13 of the bargain they had struck with Defendant.

#### 14 **FOURTH CAUSE OF ACTION**

#### 15 **VIOLATION OF NEVADA DECEPTIVE TRADE PRACTICES ACT**

#### 16 **NEV. REV. STAT. § 598, ET SEQ.**

17 92. Plaintiff repeats, re-alleges, and incorporates by reference all above paragraphs.

18 93. This cause of action is brought pursuant to the Nevada Deceptive Trade  
19 Practices Act, Nev. Rev. Stat. §§ 598 *et seq.*, (the “Nevada Act”).

20 94. Defendant is a healthcare provider that sells goods and services to the general  
21 public. Defendant’s activities are governed by the State Consumer Protection  
22 Acts.

23 95. On information and belief, affected individuals include persons over the age of  
24 60 and/or persons with disabilities.

25 96. In all requisite matters alleged herein, Defendant acted in the course of their  
26 business or occupation within the meaning of NRS §§ 598.0903 to 598.0999.

27 97. In all requisite matters alleged herein, Defendant acted willfully in violation of  
28 NRS 598.



1 98. Defendant violated NRS 598 by engaging in the unfair and deceptive practices  
2 as described herein which offend public policies and are immoral, unethical,  
3 unscrupulous and substantially injurious to consumers.

4 99. Reasonable customers would be misled by Defendant's misrepresentations and  
5 omissions concerning the security of their personally identifying information.  
6 Defendant's unfair and deceptive practices are thus likely to, and have, misled  
7 the Class Members acting reasonably in the circumstances, in violation of NRS  
8 598.

9 100. Defendant specifically engaged in the following activity and/or deceptive  
10 practices, all of which violate NRS 598:

11 a. Defendant failed to maintain and execute reasonable procedures  
12 designed to prevent unauthorized access to Plaintiff's and Class  
13 Members' personal identifying information;

14 b. Defendant acted unlawfully in storing and failing to adequately  
15 safeguard Plaintiff's and Class Members' personal identifying  
16 information;

17 c. Defendant failed to exercise reasonable care in protecting and securing  
18 their personal identifying information;

19 d. Defendant failed to properly and timely notify Plaintiff and the Class  
20 about the severity of the breach, including failure to provide an adequate  
21 description of the breach and the risks associated with the breach.

22 101. In all requisite matters alleged herein, Defendant acted knowingly within the  
23 meaning of NRS 598.

24 102. In all requisite matters alleged herein, Defendant acted willfully in violation of  
25 NRS 598.

26 103. Defendant violated, among other sub provisions of NRS 598, NRS  
27 598.0923(3) when it violated HIPPA, as discussed above.  
28

1 104. Plaintiff has been aggrieved by Defendant's unfair and deceptive practices  
 2 including because she has lost control of her personally identifying  
 3 information, and she has to expend out of pocket money and efforts to mitigate  
 4 the harm caused by Defendant.

5 105. Pursuant to NRS 598, Plaintiff and the Class Members seek a declaratory  
 6 judgment and court order enjoining the above-described wrongful acts and  
 7 practices of Defendant. Additionally, Plaintiff and the Class Members make  
 8 claims for damages, attorneys' fees and costs.

9 **PRAYER FOR RELIEF**

10 106. WHEREFORE, Plaintiff, individually and on behalf of the other members of  
 11 the Class proposed in this complaint, respectfully requests that the Court enter  
 12 judgement in favor of Plaintiff and the Class against Defendant, as follows:

- 13 • Certifying this action as a class action, with a Class as defined  
 14 above;
- 15 • For equitable relief enjoining Defendant from engaging in the  
 16 wrongful acts and omissions complained of herein pertaining  
 17 to the misuse and/or disclosure of Plaintiff's and Class  
 18 members' Private Information, and from failing to issue  
 19 prompt, complete and accurate disclosures to Plaintiff and  
 20 Class members;
- 21 • Awarding compensatory damages to redress the harm caused  
 22 to Plaintiff and Class Members in the form of, *inter alia*, direct  
 23 theft, identity theft, expenses for credit monitoring and identity  
 24 theft insurance, out-of- pocket expenses, anxiety, emotional  
 25 distress, loss of privacy, and other economic and non-economic  
 26 harm. Plaintiff and Class Members also are entitled to recover  
 27 statutory damages and/or nominal damages. Plaintiff's and  
 28

1 Class Members' damages were foreseeable by Defendant and  
2 exceed the minimum jurisdictional limits of this Court.

- 3 • Ordering injunctive relief including, without limitation, (i)  
4 adequate credit monitoring, (ii) adequate identity theft  
5 insurance, (iii) instituting security protocols in compliance  
6 with the appropriate standards and (iv) requiring Defendant to  
7 submit to periodic compliance audits by a third party regarding  
8 the security of personal identifying information in its  
9 possession, custody and control.
- 10 • Awarding Plaintiff and the Class Members interest, costs and  
11 attorneys' fees; and
- 12 • Awarding Plaintiff and the Class such other and further relief  
13 as this Court deems just and proper.

14 ///

15 ///

16 ///

**TRIAL BY JURY**

107. Pursuant to the seventh amendment to the Constitution of the United States of America and the Constitution of the State of Nevada, Plaintiff is entitled to, and demands, a trial by jury.

DATED this 7th day of January 2022.

Respectfully submitted,

**FREEDOM LAW FIRM, LLC**

/s/ Gerardo Avalos

George Haines, Esq.

Gerardo Avalos, Esq.

8985 South Eastern Ave., Suite 350

Las Vegas, NV 89123

**KIND LAW**

/s/ Michael Kind

Michael Kind, Esq.

8860 South Maryland Parkway, Suite 106

Las Vegas, Nevada 89123

*Attorneys for Plaintiff and on behalf  
of all others similarly situated*

# EXHIBIT B



1 5. ReproSource is a corporation duly organized and validly existing under the laws of  
2 the state of Massachusetts with its principal place of business located in Marlborough,  
3 Massachusetts.

4 6. As a result of the security incident described in the Complaint, ReproSource  
5 provided written notice to in excess of 220,000 individuals stating that ReproSource had been  
6 the victim of a security incident in which those customers' personally identifying information  
7 may have been accessed by an unauthorized actor.

8 7. In the aftermath of the security incident described in the Complaint, ReproSource  
9 retained Kroll Information Assurance, LLC to offer credit monitoring to all potentially  
10 impacted individuals. The value of the credit monitoring offered to all potentially impacted  
11 individuals by ReproSource was \$35.05 per-person.

12  
13 Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is  
14 true and correct.

15  
16 February 18, 2022

17 Date

*Keena M Hausmann*

Keena Hausmann

Executive Director, Privacy Officer  
Quest Diagnostics Incorporated